REMARKS

Summary of Office Action

Claims 1-5 and 11-15 are pending.

Claims 1-5 and 11-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bianco et al. U.S. Patent No. 5,048,086 (hereinafter "Bianco") in view of Ditto et al. Publication entitled "Introduction: Control and Synchronization of Chaos" (hereinafter "Ditto").

Claims 5 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bianco in view of Ditto and further in view of Lai et al. Publication SPIE (hereinafter "Lai").

Summary of Applicant's Amendments

Applicant has amended claims 1 and 11 in order to more particularly point out and distinctly claim the subject matter that applicant regards as the invention.

Applicant has added new claims 15-21 in order to more particularly point out and distinctly claim the subject matter that applicant regards as the invention.

Applicant's Response to the Rejections in view of Bianco and Ditto

Claims 1-5 and 11-15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bianco in view of Ditto.

Applicant's specification teaches two chaotic systems that stabilize onto the same periodic orbit regardless of the initial state of either system.

Bianco discusses using the difference equation $X_{n+1} = \mu X_n(1-X_n)$ to encrypt data. X_n and μ values are chosen at the encryptor and passed onto the decryptor such that the decryptor is provided with the knowledge of the initial state (i.e., X_n) of the encryptor.

Ditto is a general overview of chaotic system research.

The Examiner stated that "Bianco discloses ... [causing] the first chaotic system to assume a periodic orbit" (Office Action, page 2).

Neither Bianco or Ditto, however, show or suggest Applicant's inventions, as defined by amended claims 1 and 11, of generating the same key bitstream in two chaotic

systems independent from the initial state of either system. As a result of this independence, information about the initial state of a chaotic system does not have to be transmitted in order to synchronize the system with another chaotic system. Such a feature is advantageous in encryption because it is harder to determine the underlying mathematics of a system if no information about the underlying mathematics is actually transmitted.

More particularly, Bianco must send all of the variables (i.e., μ and X_n) used by the encryptor (i.e., $X_{n+1} = \mu X_n(1-X_n)$) to the decryptor so that the decryptor knows exactly what initial iteration (i.e., X_n) and tuning parameter (i.e., μ) was used to encrypt the data. As a result of decryptor's dependence on the initial state (i.e., X_n) of the encryptor:

> "changing the value of μ and X_n will result in a totally different sequence, allowing μ to be used as the 'key' and X_n as the 'preamble'."
> (Bianco, col. 4, lines 10-19).

In this manner, X_n is required to start the decryptor of Bianco such that X_{n+1} can be used to decrypt data. Changing the initial state to any other X will cause the decryptor of Bianco to fail. Accordingly, the encryptor and decryptor of Bianco must not only have the same initial state, but the encryptor must transmit this initial state to the decryptor in order to decrypt data.

Applicant's inventions, as defined by independent claims 1 and 11, however, generate a key bitstream by causing a chaotic system to achieve a periodic orbit independent from the initial state of that chaotic system. More particularly, the period orbit is not dependent:

> "on the initial state of the chaotic system (although the time to get on the periodic orbit can vary depending on the initial state."
> (applicant's spec, page 12)

In this manner, the initializing code of claims 1 and 11 can cause the chaotic system to assume the same periodic orbit regardless of the initial state of the chaotic system. Such an advantage may be achieved, for example, by controlling the trajectory of the system at particular points such that, over time, the system stabilizes around a particular periodic orbit. By not being dependent on an initial state, Applicant's inventions of claims 1 and 11 can decrypt data without transmitting information about the systems underlying mathematics.

In light of the foregoing, Applicant respectfully requests that the rejection of claims 1 and 11, and any claims dependent therefrom, be withdrawn because neither Bianco

or Ditto shows or suggests Applicant's inventions of claims 1 and 11 of generating a key bitstream by causing a chaotic system to achieve a periodic orbit independent from the initial state of the chaotic system. Bianco also does not show or suggest a system that assumes a periodic orbit.

Applicant's Response to the Rejections in view of Bianco, Ditto and Lai

Claims 5 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bianco in view of Ditto and further in view of Lai.

As Applicant has shown above, claims 1 and 11 are patentable. Claims 5 and 15 depend from claims 1 and 11, respectively. Accordingly, Applicant respectfully requests that the Examiner's rejection of claims 5 and 15 under 35 U.S.C § 103(a) over Bianco, Ditto, and Lai be withdrawn.

CONCLUSION

In light of the foregoing, Applicant respectfully submits that this application, including claims 1–5 and 11–15, is in condition for allowance. A favorable action is respectfully requested.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. CAOT-P02-001 from which the undersigned is authorized to draw.

Dated: September 19, 2005

Respectfully submitted,

By _____
Jeffrey D. Mullen
Registration No.: 52,056
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110-2624
(617) 951-7000
(617) 951-7050 (Fax)
Agent For Applicant